August 1990/Number 4-90

security awareness bulletin

Inside

Foreign Intelligence Threat for the 1990s

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication — Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

The Security Awareness Bulletin is produced by the Department of Defense Security Institute, Richmond, Virginia. Primary distribution is to DoD components and Federal contractors cleared for classified access under the National Industrial Security Program and special access programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and education methods.

For new distribution or address changes:

Air Force: Contact your local Publication Distribution Office.

Government agencies: DoD Security Institute, Attn: SEAT, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091, POC Del Carrell, (804) 279-5314/4223, DSN 695-5314/4223; fax (804) 279-6406, DSN 695-6406.

DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria, VA 22314-1651.

DoD contractors: Automatic distribution to each cleared facility. Send change of address to your DIS field office.

Future Threat

by Maynard C. Anderson
Assistant Deputy Under Secretary of Defense (Counterintelligence and Security)

New Perspectives for the 1990s

Chairman of the Joint Chiefs of Staff, General Colin Powell, recently stated:

"We are not going to eliminate Super Power competition from the world and we must understand that....We must protect ourselves while we take advantage of all the opportunities opened up to us by these historic changes in the world."

The "Threat" today is taking on new forms and manifestations, but it is not going to go away. Obviously, there are the threats from the "hostile" collectors of intelligence. But in addition to that, we must consider the implications of, and whether there are threats to our freedoms and way of life from things like:

- Environmental depletion—diminished mineral wealth and foreign dependence on some critical materials
- Economic factors—the balance of trade, foreign acquisition of defense industries, trends toward multinational corporations and OPEC-type groups
- Rising expectations from the Third World
- Stateless entities like the PLO
- Organized crime and international drug syndicates
- Terrorist groups
- Religious fanatics who link religion to state power
- The world's "crazies" who may have nuclear capabilities.

On this latter point, General John L. Piotrowsky, USAF, former Commander, Space Command and NORAD, speaking to the aviation/space writer association on 12 October 1989, commented, "It is chilling to consider that the Qaddafis of the world or their surrogates may be capable of holding us at risk with ballistic missiles in the coming decade..."

There are targets emerging in a new environment of ostensibly lessened conflict that need to be recognized and understood. In some cases, the counterintelligence effort in past decades has been somewhat less complex because we were dealing with known personnel in specific situations whose activities were less difficult to detect. In the future, we will be dealing with amorphous threats that are not well-defined. And in this newer situation, a euphoria of cooperation might conceal sinister purposes, intent, and capabilities that put us at a disadvantage in attempts at detection.

Our Traditional Adversary

While the threat of war among super-powers is receding, there is no reason to suppose that Soviet intelligence collection activities will cease or even become less aggressive. I look for increased efforts on the part of the Soviets to illicitly acquire unclassified western technology partly because the risk of exposure and severe penalties to the foreign intelligence service representatives are much lower than for conventional espionage.

More importantly for the Soviets, with economic problems reaching near-crisis proportions in 1989, their leadership has been grasping for ways to put their economy back on track. One strategy of course is to attempt to overcome technology lags in key industries by any possible means. Gorbachev has stated that "the historic fate of the country and the position of socialism" as well as his economic revitalization program, depend upon the infusion of new and advanced technology. The successful Soviet piracy of technology in recent times has become legendary. To maintain parity, if not superiority, the Soviets probably recognize that the real test may not be who first develops technology, but rather who is first to use it effectively.

"Increased espionage in the West is an integral part of *glasnost*" says Herb Meyer, a top CIA official under President Reagan. " It's not happening in spite of it, it's happening because of it. *Glasnost* in the Soviet Union sinks or swims on the success of *perestroika*, Gorbachev's economic restructuring. *Perestroika* rides partially on the acquisition of sophisticated western technology acquired by hook, legally, or by crook, via espionage from the West."

What is next for the Soviet Union? As recently stated by the eminent political scientist, Samuel P. Huntington, "One cannot assume that the Soviets will return to the bad old ways of the past. One also cannot assume that they will not. Gorbachev may be able to discard communism, but he cannot discard geography and the geopolitical imperatives that have shaped Russian and Soviet behavior for centuries."

Increased espionage in the West is an integral part of* glasnost. *It's not happening in spite of it, it's happening because of it.

Some analysts believe that the Soviet Union will require tougher rule to prevent its breakdown. There will be, I believe, instability in Central Europe for some time to come. On December 28, 1989, Martin Fletcher of NBC News commented: "We are a gun shot away from anarchy in any of these European nations."

Friends and Allies

It is somewhat ironic that, although the Soviet Union constitutes the greatest threat to U.S. security, the greatest challenge to the U.S. technology and industrial base will almost surely come from United States allies.

The Defense Science Board has told us under the title "The New Reality" that the advancement and application of technology has become globalized—it has replaced territory as the new coinage of world power. Exploiting new dual-use technologies will drive both economic growth and military capability in the 1990s and beyond. Asian industry is setting the pace for success in commercial exploitation of new technologies.

At one time, U.S. predominance in technology allowed Washington to strongly influence allies concerning safeguarding of information. This predominance no longer exists, and the Europeans are more and more unwilling to purchase U.S. technology if the price includes onerous rules and restrictions and is available elsewhere.

History is unkind to nations that lose control of their economic destiny. We should be prepared for both opportunities and catastrophes, either of which may strike quickly and without much warning in the days ahead. Your children and grandchildren will be compelled to remember the year 1989 in their studies of history. It marked the end of the 44 year post-war period and marked the beginning of the reconstruction of Europe.

Forecasting the Shape of the Threat

The political, economic and social environments of the 1990s are difficult to forecast because they will most likely change in ways that are not now foreseen. In a general sense, we must be prepared to "manage change."

As attitudes of confrontation between the super powers diminish, it can be expected that intelligence collection will *increase*. The dissolution of border controls allowing free passage from East to West; more opportunities for travel, education and employment by citizens of former adversary nations in Western countries; a general feeling of good will, all should contribute to opportunities for intelligence activities.

If the Central European nations and the Soviet Union are to compete with the West on an economic basis, their industrial capability must increase dramatically. Given the fact that they do not have that capability now, they must obtain knowledge and technology from available sources elsewhere. One of the most expedient and least expensive ways to do that is by theft from the West.

New Alignments and New Adversaries

The cohesion of both blocs is weakening to some extent. The North Atlantic alliance must make some changes although it will certainly remain a necessary institution. With the Eastern Bloc changes, the number of "adversaries" in terms of independent intelligence collectors targeting the United States will probably increase. Disestablishment of intelligence services, or renovation of them in some of the Bloc nations, will have a yet unknown effect on their intentions and capabilities. With American companies looking for markets in previously denied areas, exposure of Western technology will increase. Europe, anticipating economic integration by 1992, will constitute a new "bloc" economically at least, and the traditional sharing of both technology and classified information with its members by the United States must be examined in light of new, non-traditional relationships.

More neutral attitudes in Japan and the Federal Republic of Germany may become real for both economic and political reasons. There are varying degrees of regional instability in the world and seemingly increasing terrorism along with potential for Third World low intensity conflict.

The Peoples Republic of China represents a significant challenge for both United States industry and government in terms of establishing reasonable relationships at minimum risk. It can be expected that United States capabilities of all kinds will be desirable to the PRC and that American citizens of interest will be targets for exploitation.

U.S. Society and our Vulnerabilities

As an "open society," the United States offers invited or illegal adversaries opportunities to gain an advantage. White collar crime incentives, drugs, disenchantment in the work place, large numbers of immigrant workers, along with foreign exchange students and visitors, all combined with a perception by some of

our citizens that there is a lesser threat, contribute to our vulnerabilities in the '90s. And changes in East-West relations may offer an easier rationalization for some persons to commit espionage.

In government and industry, there is preoccupation with budget shortfalls and the trade deficit. There is increased foreign sourcing of supplies and foreign ownership of United States companies. There is a sort of supernational attitude of multi-national corporations and rising attention to special interests. A declining defense budget probably will require greater emphasis on U.S. intelligence activities, particularly in areas of indications and warning. Improved intelligence capabilities and activities might well serve as force multipliers while active military forces are reduced.

Responsiveness in Security Programs

The Administration is actively supporting improved counterintelligence and countermeasures efforts. In accomplishing new counterintelligence objectives, the Administration needs the assistance and cooperation of the civilian sector. Decisions must be made concerning what needs to be protected; what are the relative roles of government and industry in the future? What are the relationships between the national security and economic security? In the light of rapidly changing global forces, how can our policies be devised to retain their focus, yet be flexible?

As I mentioned earlier, managing security will mean managing change. Security professionals must be imaginative and open to new methods. What worked well in the 1980s will most likely not work well in the 1990s. We can't be afraid to make mistakes. Babe Ruth struck out 1300 times.

Specific Predictions for the 1990s

Let me offer a strategic hypothesis: the cost of espionage committed against the United States in the new decade will increase in both absolute and relative terms. Recent and continuing changes in the world enhance the opportunities for adversaries to collect intelligence causing both military and economic damage to the United States. Innovation in U.S. militarily relevant technology will continue and it will remain of interest to our adversaries. To the extent that we are successful in maintaining our edge, or indeed increasing our superiority, hostile intelligence activity will correspondingly increase.

Greed will continue as a motivation for espionage. Segments of the population, for various reasons, may not identify with the national interest and increasingly may fall prey to offers of money to support their acquired tastes and life style. Higher percentages of immigrant labor, a greater influx of foreign students, split loyalties and a pervasive view that the threat is gone will contribute to the challenge of protecting the nation's secrets.

Economic realities will seriously impact on budgets requiring a much higher level of innovative thought in the security disciplines. And we will need to get the greatest mileage out of every dollar spent. Security is not an abstraction. Security failures are identified by our counterintelligence successes in apprehending offenders. On the positive side, it is possible, and will become essential, for us to undertake systematic evaluations to measure the success of security programs. In the absence of additional stimuli like another outbreak of espionage, it is our challenge to maintain a high profile of implementing actions, resource requirements, professional capabilities, and public awareness of both problems and progress.

Security Challenges of the Future

The new structure of the "Threat" to national security information necessitates a fresh and innovative response on the part of security professionals and cleared employees alike. In plain language, what are we up against? In my opinion, the principle challenges of the 1990s are going to be these:

- What can we share with other countries without endangering our basic interests?
- How can we protect what is genuinely critical information in a time of restricted resources?
- How can we reconcile our economic interests and our security interests?

These three issues are clearly interrelated but I urge the reader to notice what is *missing* in the way these issues are phrased: a clearly defined "enemy" or "adversary" and a clearly identified body of information which warrants protection. This is the crux of the problem for us in the security business. And it demands from us a philosophical adjustment.

Yes, traditional enemies are disappearing, but the threat will never disappear. Like death and taxes, there will always be a threat! But it must be redefined to fit the new realities of our time. The new view is that we won't have easily identifiable adversaries—any nation or group could be collecting information which we would want to

The cost of espionage committed against the United States in the new decade will increase in both absolute and relative terms.

Our first task is to re-orient the intelligence and security community away from the narrow concept of the "Hostile Intelligence Threat" posed by specific intelligence services of adversary countries.

keep safe.

From Prediction to Prescription: Re-orienting Ourselves

Our first task is to re-orient the intelligence and security community away from the narrow concept of the "Hostile Intelligence Threat" posed by specific intelligence services of adversary countries. We must now see security in terms of protecting critical information from access by interests not having the authority to receive it. Foreign intelligence services which target information will continue to be a fact of life, but they constitute only one aspect of the threat.

Another task before us, and here I refer to policy makers, our nation's legislators, and security professionals, is to take a hard look at the whole classification system—in fact, all of the systems in place used to control or restrict the flow of information and technology. We need to review all of our diverse national information protection programs from Special Access Programs to embargoed technology. We can't continue to conduct each program in isolation from the others. Our resource base will be too thin to manage all of these programs concurrently.

A Coordinated Program for Security

We must consider a coordinated program in which each activity is carried out within the context of others. Someone or some authority must be able to set priorities: to determine that this or that type of information is more important than another for protecting the national interest—whether it has to do with defense, diplomacy, crime prevention, or high speed computers. For example, should not the same type of safeguarding mechanisms and penalties for disclosure which are applied to sensitive defense information similarly protect narcotics intelligence?

A comprehensive national information protection program should provide safeguards for all types of information that might, in the wrong hands, be damaging to national interests. But how to decide what needs protecting and to what degree? It boils down to a question of value. Would it be possible to establish a *damage-base system* by which the degree of protection given to information is determined by what the cost would be if that information were lost? Using this method, we could establish standards of value related to levels of classification.

There is an analogy here between safeguarding national defense information and the protection of proprietary information owned by industrial firms: In a well-managed corporation; we would expect that data, marketing plans, or trade secrets—the loss of which would threaten economic survival or corporate profit—are protected to a degree commensurate with the magnitude of financial damage that would be suffered from their compromise.

Similarly, at the national level, advanced technology (whether it is clearly defense-related or not) as well as intelligence sources and methods and defense capabilities are all national assets which deserve protection. The burden would fall to counterintelligence and security professionals in all agencies and departments of the Federal structure as well as Federal contractor facilities, working together to safeguard that (and only that) which cannot be shared at any given point in time. Somehow the decision to offer protection to a body of information must be made by some standard measure of *national interest*, and that would include economic interest.

In response to a request from the editor of the *Security Awareness Bulletin* I have shared with its readers my current thinking about security issues facing us in the new decade. Some of my personal views may not coincide with current policy. But just as certainly, I am not alone among policymakers in the Department of Defense and elsewhere in government in critically examining both established ways of thinking and time-honored programs. This intense re-evaluation, perhaps long overdue, has been necessitated by the revolutionary geopolitical events of our time and also by what we candidly expect to be a radically changing resource base for our activities.

The security of our people, our facilities, our systems and our information—the real treasure of the Twentieth Century—is a critically important function. Not because it is right in an academic, altruistic, or starry-eyed idealistic sense, but to ensure the advantage of the United States; to ensure the national security *and* to advance the national interest.

Meeting the Counterintelligence Challenges of the 1990s

A Strategic Issue Facing Our Nation

by William S. Sessions, Director, Federal Bureau of Investigation

As we emerge from the so-called "Decade of the Spy" and move into the 1990s, the U.S. Intelligence Community is faced with new realities and more challenges than ever before, the dynamics of which are unique and require highly innovative responses. Two of the realities of the 1980s were the vulnerability of the National Security Community to espionage from within its ranks and the threat posed by the volunteer. We had espionage cases involving the U.S. Military (John Walker, Jerry Whitworth, James Hall, Thomas Dolce, Bruce Ott, et al), the Central Intelligence Agency (Karel Koecher, Sharon Scranage, Larry Chin, and Edward Howard), the National Security Agency (Ronald Pelton), the private defense contracting industries (James Harper, Thomas Cavanagh, et al) and the FBI (Richard Miller), to name a few. Some of these cases resulted in grave damage to U.S. national interests. In many other cases, however, the determined work of the U.S. counterintelligence community uncovered and either significantly limited or prevented the espionage activities. These cases also forced the U.S. Government to reassess its countermeasures and security programs and reevaluate its vulnerabilities to espionage from within.

Many of the above-listed cases were the result of Americans volunteering their services to a hostile foreign intelligence service. As a result, the Intelligence Community is instituting a number of policies and operating procedures to address this aspect of the espionage threat to U.S national security.

Clearly, one lesson learned during the past decade is that countering the activities of foreign intelligence services directed against the United States, our allies, and our interests is a strategic issue that has the potential of affecting the very survivability of our Nation. The success to which we achieve this goal has both policy and resource implications to our country.

As the lead U.S. counterintelligence agency, the FBI is responsible for detecting, lawfully counteracting, and/or preventing espionage and other clandestine intelligence activities conducted for, or on behalf of, foreign powers, organizations, or persons directed at U.S. citizens, facilities, and institutions. It is also the role of the FBI to coordinate the counterintelligence activities of the other members of the Intelligence Community. As we enter the 1990s, we will be faced with new realities which will dramatically change the counterintelligence environment in which we work.

Threat Assessment and Response

One of the highest priorities in our national security strategy is the continued development of effective, efficient, integrated, and aggressive counterintelligence, countermeasures, and security programs for the United States. These programs were extensively reviewed by previous administrations and those areas identified as requiring enhancements or improvements have been identified in a variety of studies, including those set forth in a September 1986 presidential report to Congress. Although the U.S. Government has made significant progress in bolstering our counterintelligence, countermeasures, and security capabilities during the past administration, such efforts demand continued support and renewed attention. The landscape of international affairs is changing at a rapid rate, particularly in the Soviet Union, Eastern and Central Europe, as well as in the People's Republic of China (PRC). Maintaining a realistic assessment and appropriate response to the activities of the intelligence services of these and other countries is vital.

There are sweeping political changes taking place in the world. The Soviet Union through *perestroika* and *glasnost* has undertaken internal reforms and opened up to the West. Similar reforms are also taking place in Soviet-bloc countries, such as Poland and Hungary. While many political experts believe that these changes cannot be easily revoked, the student demonstrations in

Beijing on behalf of democracy, and the subsequent bloody intervention by the PRC armed forces clearly illustrate that communist governments will act in their best interests when they believe that changes are going too far.

In addition to internal reforms, nations are interacting with each other to a greater degree than ever before. In 1989, Mikhail Gorbachev visited the PRC, the first time a Soviet leader has done so for decades. Gorbachev held four summits with the Ronald Reagan administration, and in December 1987, entered into a bilateral Intermediate-Range Nuclear Forces (INF) arms reduction agreement, the first reduction of nuclear arms in world history. The warming of relations have also led to increases in immigration, exchange programs, delegations, and joint ventures between the United States and the Soviet Union. There is every indication that these trends toward improved bilateral relations will continue throughout the 1990s.

While we recognize that dramatic international changes are taking place and that world peace and reducing nuclear weapons are highly desirable goals, improved diplomatic relations do not necessarily decrease the threat to our national security from hostile foreign intelligence services. Although developments in international politics do have some relationship to intelligence activities, it is the FBI's experience that some countries actually step up their intelligence activities against the United States during times when they are making public statements about cooperation and openness. Many of the espionage subjects who were arrested during the "Decade of the Spy" actually began working for a hostile foreign intelligence service during the period of "detente" in the 1970s.

Foreign countries collect information to meet their national priorities, and these needs will continue to drive their intelligence activities, despite a warming of diplomatic relations. These countries utilize their intelligence services to collect military, political, technical, and economic information to assist in meeting their national priorities. The collection of information, particularly if it is of a classified nature, can improve their military capabilities, provide valuable insight into possible U.S. political decisions (particularly concerning bilateral agreements), and save millions of dollars in research and development programs. Effectively exploited classified information and technology can also affect the economic strength of countries.

Increased Opportunities for Espionage

The reality of the warming of relations with the Soviet Union and other communist countries is that there will be increased opportunities for their intelligence services to target, for recruitment, Americans with access to classified information and to collect valuable information on the United States. Further, during these developments, the FBI's mission to protect our Nation's security by identifying, penetrating, and neutralizing hostile foreign intelligence activities has not changed, but, in fact, has increased and is becoming more difficult.

The FBI will face a number of major foreign counterintelligence challenges as a result of the new international relationships. The first is the ever-growing presence of Soviet and Soviet Bloc nationals in the United States. Reasons for this growth are new emigration policies, arms control agreements, an increase in cultural and educational exchanges, and new investment and joint venture proposals.

During the past two years, the number of Soviet emigres has increased significantly. Looking back to 1986, less than 1,000 Soviet emigres entered the United States the entire year. In 1989, over 2,000 new Soviet emigres arrived each month. Every indication is that this number will continue to increase. In addition, the number of Soviet and East European exchange groups in such areas as academics, medicine, culture, and politics have significantly increased, as have the number of tourists and commercial visitors.

An emerging new issue of particular counterintelligence concern is expanded proposed business ventures between American enterprises and those in the Soviet Union. These potential new business ventures, which are significantly increasing, give the Soviets legitimate increased access to members of our business communities, many of whom possess classified information and/or state-of-the-art technology potentially vital to our national security. This increased access means an increased opportunity for hostile foreign intelligence services to target U.S. resources and citizens for possible clandestine intelligence collection.

Another counterintelligence challenge facing us in the 1990s is that of possible future arms control agreements between the United States and the Soviet Union. These treaties present the opportunity for the KGB and GRU to have routine access to numerous sensitive areas and individuals with classified information in the United States which, until now, were accessible only on a very limited basis.

As a result of the INF treaty signed in December 1987, the Soviets established a 13-year permanent portal site in Magna, Utah, which is staffed by up to thirty Soviet inspectors. This site is physically situated in a location which the Soviets can possibly exploit for the collection of signals and human intelligence. All Soviet personnel assigned to this location are afforded

Foreign countries collect information to meet their national priorities, and these needs will continue to drive their intelligence activities, despite a warming of diplomatic relations.

diplomatic rights and privileges. This facility was established as a verification protocol to assist in ensuring that neither side violates the terms of the treaty. The INF treaty also authorizes the Soviets to establish inspectors at three other installations in the United States for three years to witness the destruction of INF missile launchers. These three locations are Pueblo, Colorado; Marshall, Texas; and Tucson, Arizona. It is anticipated that a strategic arms reduction (START) or chemical, biological, and radiological elimination (CBR) treaty would require numerous verification permanent portal sites similar to the one in Magna, Utah. This would result in substantial increases in potential new human intelligence and signals intelligence collection platforms for the Soviets in the United States.

The challenges posed by the across-the-board increases in the Soviet presence in the United States are many. They provide the Soviet intelligence services with numerous platforms in heretofore unavailable areas from which to initiate human and technical intelligence collection operations. In fact, in the past, there have been intelligence officers, agents, and co-opted ordinary Soviet citizens among those groups who have come to the United States; many have been directed and have collected specific data while here.

Increase in Disinformation

Gorbachev's new programs of *perestroika* and *glasnost* also increase the importance of active measures operations in the United States, as well as the opportunities for them to be conducted. KGB officers, Soviet officials, and agents of influence will have greater access to elected U.S. officials at all levels, U.S. citizens, and legitimate U.S. organizations. We believe the Soviets will use this access to conduct disinformation campaigns, and attempt to manage U.S. perceptions of the current changes taking place in the Soviet Union, in order to influence U.S. public opinions, and more importantly, U.S. foreign policy. Despite Gorbachev's promise in December 1987 that Soviet disinformation programs would cease immediately, old active measures campaigns continue to resurface and new, more sophisticated, elaborate, and pervasive campaigns have been initiated.

The FBI also expects increased and aggressive intelligence operations by other hostile foreign intelligence services, especially in the area of technology transfer. As the Soviet-bloc countries open up to the West, they will need to move forward quickly in such areas as technology and research and development in order to be competitive on the international scene. If this information (much of which may be proprietary or classified) can be obtained from the United States through the efforts of their intelligence services, they can save millions of dollars in research and development. They may be able to incorporate the developments into their own research and development programs and become competitive in a much shorter period of time.

Change in Public Perceptions

In addition to the increased potential for intelligence collection by the hostile foreign intelligence services, the FBI must contend with the reality that the Soviet Union and other communist countries are no longer perceived by some elements of the U.S. public and/or the international community as an obvious threat to U.S. national security. This is clearly understood by the Soviets. Indeed, Georgi Arbatov, Director of the Soviet Institute for the Study of the United States and Canada, said it quite openly when he stated publicly, "We would deprive America of the enemy. And then how would you justify your military expenditures," and as a logical extension, a realistic and aggressive counterintelligence program. Many will thus argue that the need for spies is over. Contributing to this perception is the fact that the U.S. Government has entered into a number of bilateral exchanges with these countries, which in turn have led to an increased communist country presence in the United States. A CBS/*New York Times* poll conducted in 1989 indicated that two out of three Americans no longer consider the Soviets to be an "immediate threat," and three out of four believe nuclear war with the Soviets is unlikely.

Computer Vulnerability

What makes this shift in public perception even more troublesome is that it occurs within a society increasingly reliant on computers. Nowhere is this reliance more apparent than in the National Security Community. As computers become the primary means for communications and information exchange and storage, they represent not only a target of clandestine activity, but provide the opportunity for such activity. Unauthorized access to databanks containing national security information is very difficult to detect. Increased

reliance on computers makes security countermeasures critical.

Despite the inherent increased threat for the 1990s, to most effectively counter hostile activities of foreign intelligence services, as well as reduce security vulnerabilities, U.S. Government policies and programs for offensive and defensive counterintelligence, as well as physical, technical, personnel, counterimagery, operational security and information security must be systematically strengthened and made mutually supportive. Moreover, current and anticipated budget constraints in the U.S. Government and the FBI dictate the need to identify our most critical vulnerabilities and apply the appropriate attention and remedies to eliminate them.

Cooperative Effort

Regardless of these anticipated fiscal constraints, the FBI, as the lead national counterintelligence agency and working in conjunction with the counterintelligence components of other Intelligence Community agencies, must continue to take the necessary steps to address the evolving hostile foreign intelligence threat in the 1990s. We are continuing to facilitate the exchange of counterintelligence information with other Intelligence Community members, assisting in developing their counterintelligence training programs, and assigning FBI Special Agents to the counterintelligence components of other Government agencies in national policy formulation positions. It is essential that our efforts compliment rather than duplicate each others'. Our ability to collect and analyze information is essential to our efforts, especially in implementing our national counterintelligence strategy and priorities. With the current realities in the world, it will be even more critical to fully identify and articulate the intelligence threat to U.S. policymakers, the Congress, and the U.S. public.

To best serve the policymaking and resource allocation levels of the U.S. Government, the FBI must continue to collect, analyze, and successfully exploit the hard information on hostile foreign intelligence activities directed against the United States. U.S. national foreign policymakers and Congress, in turn, must act upon this information, when warranted, and ensure that U.S. counterintelligence concerns are considered when formulating, funding, and implementing national foreign policy.

The FBI relies heavily on information from the public in fulfilling its counterintelligence mission. With the reality that a portion of the American public may no longer perceive the Soviet Union and other communist countries to be an obvious military threat to U.S. national security, we will be challenged to clearly explain the genuine seriousness and tenacity of the hostile foreign intelligence services' threat to the United States, its institutions, facilities, and its citizens. In doing so, it must be made clear to the public that our purpose is to protect U.S. national security, enhance peace and understanding, and not to discourage improvements in relations between the United States and the rest of the world.

The 1990s will present increasing new challenges to the Nation and the U.S. Intelligence Community. Through an integrated effort and dedication, the FBI will continue to meet its responsibilities, and perform its duties in the area of foreign counterintelligence.

Looking back to 1986, less than 1,000 Soviet emgires entered the United States the entire year. In 1989, over 2,000 new Soviet emigres arrived each month.

Intelligence Issues of the new Decade

By William H. Webster, Director of Central Intelligence, from remarks made to the Baltimore Council on Foreign Affairs, February 20, 1990

I would like to focus on some of the recent changes in Eastern Europe and the Soviet Union, and the intelligence issues we face in the new decade. I am convinced that intelligence—which is after all information about the plans, the intentions and the capabilities of other nations—is critical in this period of change. And I want to tell you about our continuing counterintelligence concerns, which, I believe, will take on even more importance in protecting our national security well into this decade. Our national policy will be determined to an even greater extent by changes occurring throughout the world—changes which will affect everything from the defense budget and foreign aid to how best to share our expertise and advance the institutions of democracy.

By the middle of this year, the political landscape in Eastern Europe will have again changed dramatically as all six of the Warsaw Pact countries plan to hold national and local elections. Elections will bring key issues to the fore but they do not guarantee an easy transition from Communism. They will have to be accompanied by tough reforms—reforms that will bring home the hardship of unemployment, higher food prices, and inflation to a population whose shelves may have held very little, but what was there had been heavily subsidized. Reformist governments will also have to be responsible to people who will demand that the economic burden be equitably shared.

There is no perfect model for transition in Eastern Europe—what is happening there is unprecedented. And while these countries face similar problems, each will go through a different transition process that reflects its unique history and individual ties to the West.

But a key factor in all of Eastern Europe will be what happens in the Soviet Union. The Soviet Union shares the challenges of reform that the Eastern European countries are facing—it, too, is undergoing unprecedented change. Given its tremendous size and its cultural diversity, its historical and political experience, the challenges for the Soviet Union will be even greater.

For the intelligence community, the immediate task is to look at the decrease in the Soviet and Warsaw Pact threat to Europe. Over the last year, the Soviets have unilaterally reduced their forces in the European theater, and even greater reduction is likely as Soviet forces are withdrawn from Hungary, Czechoslovakia and Poland.

We are going into a new world of defense spending, and President Bush has asked us to look at the changing nature of the threat and to determine how it affects our national security. We know that the Soviet strategic forces continue to be modernized and their military research and development programs continue to receive generous funding. And we still must reckon with a continuing Soviet effort to enhance its influence around the world For these reasons alone I think we must maintain a strong intelligence community.

At the same time, counterintelligence—our need to know what other countries want and their means of getting it—remains critical for us. And in the 1990s, as countries focus more on economic competitiveness, what will be sought is sensitive information that will give a country a competitive edge.

The means of getting this information can be relatively simple when one considers that foreign investors who buy into American industries could have access to sensitive U.S. technology. Earlier this year, President Bush moved to nullify the recent sale of a civilian aircraft parts-manufacturing firm to an arm of the Chinese government. His decision was based, in part, on evidence that the buyer involved had previously tried to gain access to sensitive technology in this manner.

Attempts to acquire sensitive technology by all nations is increasing and becoming more sophisticated. But in this new political climate—a climate where the enemy is not clearly defined—we expect collection activities to become more selective.

I would like to make a few observations at this point about counterintelligence because I think it is important to understand what has changed and what has not. I think the KGB has become less confrontational in the sense that they avoid doing blatant or flat-footed things that could create a major press issue. But the activity is there and it will continue. Within the Soviet Union, however, there does seem to be a movement toward relaxing KGB repression of Soviet dissidents.

As for the Eastern European intelligent services, their subservience to the KGB and the GRU is due for careful review. Several countries are already talking about making their intelligence services work for national interests rather than those of a second party. In Hungary, for example, the Foreign Ministry publicly disassociated itself from the Clyde Lee Conrad affair and declared that this was an erroneous policy pursued by the previous leadership without regard to the country's national interest. Conrad, a former U.S. Army sergeant, was arrested in West Germany in the summer of 1988 and charged with stealing NATO secrets. He had been recruited and handled by a Hungarian intelligence officer.

But I think it is important to remember that espionage and counterintelligence are widely recognized in Eastern Europe as necessary functions, and the apparatus for this work is likely to remain in place. The intelligence and counterintelligence services will be reorganized and resubordinated, in may cases, to newly elected masters instead of the party bosses, but the work will continue.

Additionally, the Warsaw Pact treaty commitments require East European intelligence services to cooperate with the Soviets, and this is going to provide mission continuity, especially when it is consistent with the national interest of the countries involved. And so I don't expect military intelligence collections efforts to abate—certainly not in the near future. The internal services—the secret police, on the other hand, are in turmoil and political reform will likely bring significant change to these once formidable organizations. In fact, it is safe to say that the East German internal services are dying.

The new political leadership in Eastern Europe will also bring in new oversight mechanisms. We hope oversight will reduce some hostile intelligence activity—such as passing sensitive technology to the Soviets—an activity which is incompatible with requests for U.S. loans. But fundamental changes in intelligence missions are not likely while the Warsaw Pact treaty connections are still in place. Moreover, the current generation of foreign intelligence managers—all picked form old Communist loyalists and trained in the Soviet Union—represent a substantial source of expertise that many prove difficult to replace.

While intelligence works to protect U.S. secrets, we are also alert to the effects of change. While there are certainly risks in a time of change, the greater risk for our nation is in not participating in its opportunities. Change has brought increased economic opportunity for the people in Eastern Europe and for Western commerce. But the United States in the 1990s will not be the only, nor perhaps the major, player participating in rebuilding the economies of Eastern Europe. The new leaderships in Eastern Europe will look to Western Europe and to Japan to play key roles in shaping their future.

Our responsibility to protect democracy also extends to the area of arms control. It is the job of intelligence to monitor the treaties before us and to be ready when the negotiations now on the table are concluded. The resource implications of this are serious. Reducing conventional forces in Europe—now an accepted and essential part of the changing political landscape—involves negotiations between 23 countries. It encompasses all forces between the Atlantic Ocean and the Ural mountains and includes both ground forces and air forces. But such is the rapid pace of change today that a number of negotiations—even those which are as complex as CFE—may be concluded within the year.

Through monitoring arms control agreements, identifying counterintelligence efforts, advising on the risks and the opportunities of rapid change throughout the world, intelligence has moved ahead into the next decade. But the spirit of freedom which has swept through Eastern Europe and into the Soviet Union has confounded all attempts to measure change. The forces now unleashed will propel us into the next century, and in spite of the threat of terrorism, of weapons proliferation, of narcotics, of ethnic rivalries and economic pressures, we could not hope for more auspicious or more momentous times. What will history say of how we responded to these times? The ultimate answer is beyond our intelligence systems. It lies in the hearts and the will of all who cherish the blessings of liberty for ourselves and our posterity.

A View from Industrial Security

An interview with Greg Gwash, Defense Investigative Service, Director for Industrial Security, Pacific Region, on the changing intelligence threat

(After this interview took place, Mr. Gwash was selected to become the new DIS Deputy Director for Industrial Security.)

Q: Mr. Gwash, what do you think are the real Security and Counter-espionage challenges of the 1990s?

A: We have to look at the changing situation today to see where things are going. Today, opinion polls cite international drug trafficking, not nuclear war, as the principal threat and the majority of the American public also rate violent crime and the budget deficit as greater threats to U.S. security than Soviet aggression. I think public perceptions may not be far off the mark.

Clearly, the Hostile Intelligence Officer—hiding behind every other bush or under every other bed—is not America's foremost concern. Our real challenge in the 1990s is how do we as security professionals remain credible and viable with both an actual decrease in funding and what some people argue to be a decrease in the reason or rationale for our professional existence?

Q: Do you have any ideas you'd like to propose?

A: Here are a couple of ideas: First, on the issue of CREDIBILITY: We need to stop simplifying the present situation by saying things like "even though the situation appears different today, nothing has really changed." The situation *is* different today and we security professionals are the ones who are not changing!

Yes, I know foreign governments continue to collect against us and indicators point to increases in attempts to collect military and economic intelligence. But—the framework for national, regional and international competition is different today, and not just because of the metamorphosis of Eastern Europe or Gorbachev's *perestroika.*

Q: Are you saying that the hostile intelligence threat has radically changed?

A: Actually, I think we need to stop directing our audience's attention to just "hostile intelligence" activities as THE THREAT.

The threat is broader than that, and the term itself may be obsolete. I believe our *credibility* depends on a more sophisticated analysis and presentation to the public of the many-sided problems of Information Security, Personnel Security and Technology Transfer.

Q: How can we meet these new challenges in the face of shrinking resources?

A: That has to do with our VIABILITY—Our limited resources today and in the future cannot safeguard everything in Pandora's Box—from ceramic manufacturing process (Hardly an emerging technology—wasn't pottery first invented by Neanderthal Man?) to things like super conductors and nuclear triggers which demand protection.

The Government must decide *what* to safeguard and *what* to release. We cannot continue to classify indiscriminately or withhold the release of common technology from the rest of the world. The recent meeting of COCOM which resulted in a major reduction in the number of controlled technologies is an important step in this direction.

Security professionals must be allowed to focus their limited resources on the protection of *properly* classified information and on that critical technology which truly supports our national security.

Q: OK, we can carefully limit the scope of what is to be protected, but what about cost-effective countermeasures?

A: The second part of the *VIABILITY* equation is the recognition that the single common denominator we share with those collecting against us is the TARGET! Our personnel security programs must be recognized as *far more important* than steel safes, electronic alarms or, perhaps worst of all, expensive TEMPEST countermeasures.

The development of Security Awareness programs and effective training products such as *ESPIONAGE 2000* and *Espionage Alert** are only the beginning of our job. We also need *timely* periodic reinvestigations of our cleared personnel and we need to get *beyond mere compliance* in the defense contractor's implementation of personnel security practices. And, we need quicker adjudication of personnel security issues which will preserve due process, but not drag on so long that we're locking the barn door *after* the horse is long gone.

Q: Do you believe we can actually meet these objectives in the 1990s?

A: Yes, I believe there is reason for optimism. There is strong evidence that Government and Industry can *work together* to maintain effective counterintelligence and security.

One recent initiative which I hope will help *concentrate* our limited resources and become a springboard for future successes, is The National Industrial Security Program—the NISP—a proposal to merge our many and diverse industrial security programs into a single *unified, cohesive* and *affordable* program.

The President of the United States has recently directed further study and review of the NISP. Both policy leaders in the Department of Defense and the principal managers of the Defense Investigative Service fully support the concept.

Q: Streamlining of government programs might save a lot of money, but what can be done at the local level?

A: Better cooperation among defense contractors supported by government might be one answer. A good local example has been the creation here in Los Angeles of the Industrial Security Awareness Council—ISAC for short—consisting of representatives of many local defense and aerospace firms, the FBI, and the Defense Investigative Service.

The ISAC was chartered in 1988 *to promote security awareness* and thereby reduce industrial vulnerability to espionage, as well as conserve resources by eliminating duplication of effort. The combination of resources from industry, the FBI, and DIS has resulted in some outstanding achievements, including awareness videos and posters, and an ongoing training seminars for new FSOs and security staffers. It's an idea whose time has arrived and *both* the FBI, thru its National DECA Coordinator (Rusty Capps) and DIS, thru our Deputy Director for Industrial Security (Bob Schwalls), are promoting the establishments of ISAC-type organizations nationwide.

Q: It looks like an essential ingredient in this formula for survival and success is a close working relationship between security and counter-intelligence professionals.

A: Definitely yes, The cooperation between counterintelligence and security professionals in government and industry has never been better than it is today. We are facing these radical changes from a position of strength. However, suffice it to say, in this business we're in today we need to remain mindful of the fate of the dinosaur—Counterintelligence and Security must *evolve* together in this new environment or like the dinosaur, we will surely find ourselves extinct! I am confident we will not let that happen. There is too much at stake.

* *Espionage 2000* (produced by Hughes Aircraft and the FBI) and *Espionage Alert* (produced by Northrop Corporation) are two completed security awareness video products which are available through FilmCommI and DIS regional E&T specialists.

Presenting Believable Arguments:

A Discussion For Security Educators

by Dr. Lynn F. Fischer, Chief, Security Awareness Division, Department of Defense Security Institute

Our Credibility under Attack?

Security staff who spend a good part of their time providing briefings and other types of awareness training are gearing up to field such questions as, "If the Soviet Union is undergoing a political upheaval that may lead to a Western-style democracy, why would the Russians continue to pose an intelligence threat to the United States?"; "Don't the dramatic changes in Eastern Bloc countries mean that their intelligence services will no longer target U.S. citizens overseas?"; or, "With the end of the Cold War, is there really a need for all these procedures to safeguard classified material?" How we answer these questions will affect our credibility as promoters of security programs in government and industry.

For most Americans, the lessening of the military threat and the breakup of monolithic communism seems almost too good to be true. Optimism about the future is running high, and in the current, relaxed atmosphere there is a popular view that the idea of being targeted for espionage is a thing of the past. Based on the discussions by Mr. Anderson, Judge Sessions, and Judge Webster in this issue, it's quite clear that the threat is still very much with us—if not greater than before. As security educators we must be able to establish this fact in the minds of our target audience and respond to critical questioning of our security requirements in ways which clearly make sense. The material in this and future issues of the *Bulletin* is intended to directly address this special need of security professionals by providing facts and well-reasoned, intelligible arguments for continued vigilance and good stewardship in the protection of classified and sensitive information.

Making sense out of a complex situation:

FBI Director William S. Sessions explicitly spells out for us why the foreign intelligence threat for the 1990s appears to be more ominous than before. A renewed threat is occurring at the same time that international public opinion perceives that there has been a dramatic reduction of Cold War tension and military confrontation between the major world powers. As Judge Sessions explains, there is a close relationship between the threat and public opinion. A popular view that political and military tensions have been relaxed promotes easier access to critical and defense-related information by groups and organizations who would use it to damage our national interest.

In our leading article, Mr. Anderson, at OSD Policy, stresses Soviet intensification of efforts to obtain United States technology to strengthen their faltering economy. In fact, quoting a former CIA official, increased espionage, particularly that which targets advanced technology is a direct consequence of *glasnost* and *perestroika.* We can expect intensified efforts to recruit U.S. citizens at home and abroad as sources for all kinds of sensitive information, particularly, technology which may ultimately be used against us.

This assertion is backed-up by CIA Director William H. Webster who recently stated in a speech at the National Press Club: "Around the world, our stations are reporting more aggressive actions, more robust intelligence collection efforts and more efforts to recruit our embassy and our intelligence personnel than we have seen in a long time."

Ironically, conventional wisdom reflects just the opposite view: that a decrease in the military threat and an easing of tensions means a corresponding decrease in the foreign intelligence threat. This, of course, is a fallacy which we as security educators must be able to puncture with ammunition provided by people "in the know" such as Webster, Sessions and Anderson. We can also point out at least one lesson from recent history: the period of *detente* in the 1970s (when cold war hostilities were also at a low ebb) coincided with an espionage offensive by Soviet Bloc intelligence services. It was during this period of relaxed vigilance that two of the most damaging spy ring operations in history were at their highest level of activity: Walker/Whitworth and Conrad (in Europe).

Identification Friend or Foe?

As pointed out by Maynard Anderson and Greg Gwash, we are, in terms of technology targeting, being threatened by potential adversaries and *also* nations we have come to consider as allies. At the interpersonal level, most of us expect open and honest behavior by friends, and covert, deceitful actions by enemies. Many people are surprised when it doesn't work out that way at the international scene. Possibly one of the big adjustments we as security educators are faced with is the need to describe the world in less simplistic terms. When it comes to protecting critical information, it's no longer a case of the Soviet Bloc against the Free World or, friends vs. enemies—it never was in fact that simple.

Some forty years ago, a prominent scholar in the field of international relations, Hans Morgenthau, called for "political realism" in trying to make sense of what other countries or their governments are doing. In his controversial book, *Politics Among Nations*, Morgenthau argued that nations, in the conduct of their international or commercial affairs are (and should be) motivated by self-interest regardless of high-sounding or moralistic rhetoric. "Interest" is equated with power and wealth—that's the name of the game. We shouldn't expect statesmen or intelligence organizations as instruments of the state to betray that basic value.

The point is, each nation is a friend when there are interests in common—and likewise, a potential adversary, when there are not. Interests are in conflict when we chose to withhold information or technology which another country or organization desires to improve its national economy or defensive posture. Some people were shocked by Morgenthau's "realism" when he published his work in 1948. But we should not, nor should we be caught off-guard when we read news reports that the intelligence service of a friendly nation has been targeting one of our largest computer corporations for several years or, as in the case of Jonathan J. Pollard, agents of a close ally penetrated the security of U.S. Naval Intelligence. Political realism as it applies to the real world of security is an idea that is well worth sharing with our employee populations.

Taking "Selling Security" Seriously

In recent months, a great deal of favorable discussion has been heard about Joseph A. Grau's *Bulletin* feature on "Selling Security" (May, 1989)—the need to adapt product-marketing techniques and strategies for selling ideas to enhance motivation and security awareness. Part of Joe Grau's discussion concerned maintaining the credibility of the communicator. Credibility, he states "means that people must trust you and believe in your competence enough to respect and accept your judgment." Technical competence and, just as important, the appearance of technical competence is essential to establish this trust. In other works you must "know your product." Applying this idea to selling personnel on the reality of the threat, your credibility as communicator is ensured by the use of pertinent, and up-to-date information and by your ability to use that information to justify and advocate specific security procedures and countermeasures.

Up to now our security programs and security education efforts have been driven by a common understanding of the reality of the foreign intelligence threat. We can see in the public statements of both CIA and FBI directors, as well as Pentagon policy makers, an attempt to redefine that threat in terms of national interest. Their statements identify for us those things which have not changed and those which may. Obviously, the impact of our "sales-pitch" and of our security programs in the 1990s rests on our ability as educators to bolster our credibility by backing up (with solid information) the reality of a continuing intelligence and foreign-interest threat aimed at critical information and technology. What follows are five practical suggestions for communicators who are coming to terms with this new reality.

Advice to Consider when Selling Security

1. **Establish your credibility with the best facts available:** Whenever possible support your statements about the foreign threat by citing recognized authorities: official government publications, reputable public media, or "experts" as sources of key facts and interpretations of current events. Let's face it, mention the name of a leading public figure whom we know to have direct access to the most reliable information about security or counterintelligence and ears prick up. As you see, in this issue of the *Bulletin*, we have taken our own advice. Speeches or interviews by public officials are often available through their agency's public affairs office or are reported in leading newspapers and magazines. In briefings, company newsletters, or other security awareness training aids which you produce for local use, it is not necessary to restrict your information to that which appears in official government sources so long as you (1) cite the source of the information and (2) are careful not

to suggest that it has been officially verified or confirmed by the U.S. Government.

2. **Exploit media sources for all their worth for useful information.** For the present, the availability of unclassified, up-to-date reports from our intelligence and counterespionage organizations to support security education is very limited. We hope that this will change in the future, but until then, leading public media correspondents can help fill the gap. Some of the best at present include Michael Wines, reporter for the *New York Times*, Bill Gertz, *Washington Times*, Bob Adams, *St. Louis Post-Dispatch*, and Ronald J. Ostrow for the *Los Angeles Times*. You may come to rely on others who are equally helpful about facts and interpretations about the espionage threat and foreign groups targeting U.S. technology. Your agency or firm may already subscribe to an on-line information retrieval service such as Lexis-Nexis from Mead Data Central, DIALOG, or Dow Jones News/Retrieval. With the use of search keywords, like "espionage, foreign intelligence," or "counter-intelligence," recent articles and news reports can be identified and retrieved in abstract or full-text form. (Federal agencies can contract for the use of any of these services through the Library of Congress FEDLINK system).

3. **Seek out counter-intelligence professionals for support.** A close working relationship between security educators and counterintelligence professionals within and across agencies will become even more indispensable for effective security education. The CI people can tell us what is happening; and ultimately, it is to these sources which we turn for solid information about the multi-faceted threat. For several years, a very bright spot in this developing relationship has been the Federal Bureau of Investigation's DECA (Development of Espionage and Counterintelligence Awareness) briefing program for defense contractors. These briefings are now available to federal agencies and field components. Classified and unclassified DECA briefings are provided by FBI agents to cleared contractor facilities to enhance awareness of cleared employees. DECA briefings can be arranged by request to FBI field offices.

4. **Get the most out of training products which are already available in industry and government.** Major defense contractors and agencies and departments of the Federal Government produce (principally for their internal use) video products, posters, briefing packages, publications and other types of training aids to support security programs. Increased efforts are being made by the Defense Security Institute, regional organizations of defense contractors, and interagency groups within government to promote a broader distribution and use of these products. As new items become available, special notices will appear in the *Security Awareness Bulletin.* These will be listed, with information on how to purchase or borrow, in our publication, *Training Aids for Security Awareness.* You may decide not to use a product as it was originally produced since many include agency or company-specific content. However, it still may be extremely helpful. It may give you some great ideas about graphics, attention-grabbers, wording, or it may contain valuable factual information or quotable quotes from public officials that could be plugged into your own briefings or training vehicles. The point is, most of these products are very expensive to produce—particularly videos and posters—and it is in everybody's interest to get the optimum degree of exposure out of each product regardless of origin.

5. **Be well-informed and responsive to new developments.** Who knows for sure what is coming down the pike? Things are happening so fast that one risks being "out of date" each time a threat briefing is delivered. Where real changes take place in the structure or source of a threat we must be alert and responsive to that change, but also be well informed enough to spell out its underlying consequences. Let's take a current example: The dismantling of the East German Intelligence Service will rid us of one of the most formidable intelligence organizations in Europe—in the past noted for its instigation of such cases as James Hall (1988), Ernst Forbrich (1984), Francisco de Assis Mira, and Alfred Zehe (1983). However, it hasn't happened yet and when it does, there are strong indications that its resources will be absorbed by Soviet services which have invested heavily in the training of East German personnel. The message for personnel stationed in Europe may be that the more things change, the more they remain the same. Once again, keep an eye out for officially released information and for media reports, especially from highly reputable journalists at the scene of events.

Forging ahead with new methods and approaches

Mr. Anderson has urged us to be imaginative and open to new ways of doing things in our security programs. For the security educator, this could be translated into breaking with old traditions, such as the tradition of "meeting" requirements by delivering a set number of formal security briefings and thereby feeling content that we have successfully completed our tasks. Or it

could mean revamping all of the "threat" material presented to cleared employees to bring it in line with the stronger emphasis on the vulnerability of advanced technology or with the more complex view about where the threat is coming from. Whatever adopting new methods may mean to individual security professionals who are given the responsibility for security education, it is clear that each one of us has been presented with a unique challenge and with the opportunity to be creative, even experimental. I hope your reaction to the changing security environment agrees with the sentiment expressed by one new security staff member who said, "This job is beginning to look interesting."